Composante du produit n° 85-002-X au catalogue de Statistique Canada
Juristat

Article de *Juristat*

Les incidents autodéclarés de victimisation sur Internet au Canada, 2009

par Samuel Perreault

Diffusé le 15 septembre 2011

Statistique Canada Statistics Canada

Canada

Comment obtenir d'autres renseignements

Pour toute demande de renseignements au sujet de ce produit ou sur l'ensemble des données et des services de Statistique Canada, visiter notre site Web à www.statcan.gc.ca. Vous pouvez également communiquer avec nous par courriel à infostats@statcan.gc.ca ou par téléphone entre 8 h 30 et 16 h 30 du lundi au vendredi aux numéros suivants :

Centre de contact national de Statistique Canada

Numéros sans frais (Canada et États-Unis) :

Service de renseignements	1-800-263-1136
Service national d'appareils de télécommunications pour les malentendants	1-800-363-7629
Télécopieur	1-877-287-4369

Appels locaux ou internationaux :

Service de renseignements	1-613-951-8116
Télécopieur	1-613-951-0581

Programme des services de dépôt

Service de renseignements	1-800-635-7943
Télécopieur	1-800-565-7757

Comment accéder à ce produit

Le produit n° 85-002-X au catalogue est disponible gratuitement sous format électronique. Pour obtenir un exemplaire, il suffit de visiter notre site Web à www.statcan.gc.ca et de parcourir par « Ressource clé » > « Publications ».

Normes de service à la clientèle

Statistique Canada s'engage à fournir à ses clients des services rapides, fiables et courtois. À cet égard, notre organisme s'est doté de normes de service à la clientèle que les employés observent. Pour obtenir une copie de ces normes de service, veuillez communiquer avec Statistique Canada au numéro sans frais 1-800-263-1136. Les normes de service sont aussi publiées sur le site www.statcan.gc.ca sous « À propos de nous » > « Notre organisme » > « Offrir des services aux Canadiens ».

Des corrections ont été faites dans ce produit.

La publication a été remplacée le **5 juin 2013**.

Veuillez prendre note du (des) changement(s) suivant(s):

Note aux lecteurs
En raison de la déclaration incorrecte du nombre d'affaires de pornographie juvénile par un service de police pour les années 2008 à 2011, les données qui figuraient au départ dans le présent rapport ont été supprimées.
Les données révisées sont disponibles dans les statistiques de la criminalité de 2012, publiées le 25 juillet 2013.

Nous regrettons les inconvénients que cette situation peut avoir causé.

Statistique Canada
Juristat

Les incidents autodéclarés de victimisation sur Internet au Canada, 2009

Publication autorisée par le ministre responsable de Statistique Canada

© Ministre de l'Industrie, 2011

Tous droits réservés. Le contenu de la présente publication électronique peut être reproduit en tout ou en partie, et par quelque moyen que ce soit, sans autre permission de Statistique Canada, sous réserve que la reproduction soit effectuée uniquement à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé destiné aux journaux et/ou à des fins non commerciales. Statistique Canada doit être cité comme suit : Source (ou « Adapté de », s'il y a lieu) : Statistique Canada, année de publication, nom du produit, numéro au catalogue, volume et numéro, période de référence et page(s). Autrement, il est interdit de reproduire le contenu de la présente publication, ou de l'emmagasiner dans un système d'extraction, ou de le transmettre sous quelque forme ou par quelque moyen que ce soit, reproduction électronique, mécanique, photographique, pour quelque fin que ce soit, sans l'autorisation écrite préalable des Services d'octroi de licences, Division de la gestion de l'information, Statistique Canada, Ottawa, Ontario, Canada K1A 0T6.

Septembre 2011

N° 85-002-X

ISSN 1205-8882

Périodicité : irrégulier

Ottawa

This publication is also available in English.

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population, les entreprises, les administrations canadiennes et les autres organismes. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques précises et actuelles.

Signes conventionnels

. indisponible pour toute période de référence
.. indisponible pour une période de référence précise
... n'ayant pas lieu de figurer
0 zéro absolu ou valeur arrondie à zéro
0^s valeur arrondie à 0 (zéro) là où il y a une distinction importante entre le zéro absolu et la valeur arrondie
^{p} provisoire
^{r} révisé
^{x} confidentiel en vertu des dispositions de la *Loi sur la statistique*
^{E} à utiliser avec prudence
F trop peu fiable pour être publié

Les incidents autodéclarés de victimisation sur Internet au Canada, 2009 : faits saillants

- Selon les résultats de l'Enquête sociale générale de 2009, environ 7 % des internautes adultes ont fait l'objet de cyberintimidation. La proportion touchée était semblable chez les hommes et les femmes.
- Le risque de cyberintimidation était plus élevé chez certaines personnes, dont les jeunes adultes (18 à 24 ans) (17 %), les célibataires (15 %) et les abonnés de sites de réseautage social (11 %).
- Environ 4 internautes adultes sur 10 (40 %) ayant fait l'objet de cyberintimidation ont été ciblés par un étranger. Les hommes (46 %) étaient légèrement plus susceptibles de faire l'objet de cyberintimidation d'un étranger que les femmes (34 %).
- Un peu moins de 1 adulte sur 10 (9 %) a déclaré un incident de cyberintimidation contre au moins un enfant dans son ménage ou 2 %, un cas de leurre d'enfants. La plupart (71 %) des adultes ont dit que l'enfant victime de cyberintimidation était une fille.
- Une proportion relativement petite des incidents de cyberintimidation ont été signalés à la police. Toutefois, les incidents contre des enfants ont plus souvent été signalés que ceux visant des adultes (14 % par rapport à 7 %).
- Environ 4 % des Canadiens ayant utilisé Internet au cours des 12 mois précédents ont indiqué avoir été victimes de fraude bancaire par Internet.
- Les internautes vivant dans les régions métropolitaines de recensement étaient plus susceptibles que ceux vivant à l'extérieur de celles-ci de déclarer des incidents de fraude bancaire par Internet (4 % par rapport à 2 %).
- Le risque de fraude bancaire par Internet augmente en fonction du revenu personnel. Les internautes touchant un revenu supérieur à 60 000 $ étaient trois fois plus susceptibles d'être victimes de fraude bancaire par Internet que ceux qui gagnaient moins de 20 000 $ par année.
- Environ 14 % des internautes qui ont effectué des achats en ligne au cours des 12 mois précédant l'enquête ont éprouvé des problèmes. Ces types d'incidents comprenaient surtout les suivants : les produits ou services n'ont pas été livrés même s'ils ont été payés d'avance; les produits ou services reçus n'étaient pas ceux décrits sur le site Web; et des sommes supplémentaires ont été retirées du compte sans autorisation.
- Les deux tiers (65 %) des internautes ont affirmé que leur ordinateur avait déjà été infecté par un virus, un logiciel espion ou un logiciel publicitaire. En outre, 4 internautes sur 10 (39 %) ont indiqué avoir fait l'objet d'au moins une tentative d'hameçonnage.
- Un internaute sur 6 (16 %) a indiqué qu'il était déjà tombé sur du contenu faisant la promotion de la haine ou la violence. Dans la plupart des cas, ce contenu visait des groupes ethniques ou religieux.

Les incidents autodéclarés de victimisation sur Internet au Canada, 2009

par Samuel Perreault

De plus en plus de Canadiens utilisent Internet régulièrement (Middleton, 2010). Selon les résultats de l'Enquête canadienne sur l'utilisation d'Internet, 8 ménages canadiens sur 10 avaient accès à Internet[1] (Statistique Canada, 2011). Toutefois, l'avènement des nouvelles technologies de l'information entraîne aussi de nouvelles opportunités criminelles et de nouveaux risques de victimisation (Gendarmerie royale du Canada, 2011; Sécurité publique, 2011). Ces dernières années, les gouvernements et les institutions, de même que les utilisateurs, ont reconnu le besoin de s'attaquer à la question du risque de victimisation sur Internet (Kowalski, 2002). Toutefois, à ce jour, il demeure difficile d'évaluer la nature et l'étendue du problème. Les données policières nous fournissent certains renseignements, mais les données déclarées par les victimes indiquent que seulement une faible proportion des incidents de victimisation sont signalés à la police (Perreault et Brennan, 2010).

En 2009, l'Enquête sociale générale (ESG) sur la victimisation a été menée auprès des Canadiens de 15 ans ou plus résidant dans les provinces. Pour la première fois, l'ESG a permis de recueillir auprès des Canadiens de l'information sur leurs perceptions et leurs expériences en ce qui concerne la victimisation sur Internet, notamment la cyberintimidation, la fraude bancaire par Internet, et les problèmes concernant les achats sur Internet (voir l'encadré 1).

Le présent article de *Juristat*[2], qui a été élaboré à partir des données de l'ESG, fournit de l'information concernant la victimisation sur Internet, telle qu'elle a été déclarée par les Canadiens. En particulier, on y analyse les caractéristiques sociodémographiques et économiques des victimes (comme l'âge, le niveau de scolarité et le revenu) et les caractéristiques de l'utilisation d'Internet de celles-ci. On y traite aussi des préoccupations des internautes canadiens concernant la sécurité et du contenu haineux trouvé sur Internet.

Encadré 1
Définition de la victimisation sur Internet

Les définitions suivantes ont été formulées à partir des questions posées aux répondants de l'Enquête sociale générale de 2009. Il convient de mentionner que les données provenant des réponses à ces questions sont fondées sur les perceptions des personnes et ne devraient pas être comparées avec les données déclarées par la police qui peuvent mesurer des concepts semblables.

Cyberintimidation : A déjà reçu des messages menaçants ou agressifs ou été la cible de commentaires haineux envoyés par courriel ou messagerie instantanée, ou affichés sur des sites Internet; l'envoi de courriels menaçants en utilisant l'identité de la victime.

Leurre d'enfants : A déjà été leurré ou a reçu des avances sexuelles en ligne, par exemple, dans un courriel, un message instantané ou un salon de clavardage. Bien que la plupart des cas de leurre d'enfants pourraient être considérés comme tels selon la définition du *Code criminel,* certains pourraient ne pas l'être, selon l'âge de la victime ou du contrevenant et les circonstances.

Fraude bancaire par Internet : Au cours des 12 mois précédant l'enquête, un utilisateur d'Internet s'est servi d'une carte de crédit ou de débit (ou des détails de la carte) pour effectuer des achats ou retirer des fonds du compte sans l'autorisation du détenteur de la carte.

Problèmes concernant les achats en ligne : Au cours des 12 mois précédant l'enquête, achats de produits ou services qui n'ont jamais été livrés alors qu'ils avaient été payés d'avance; produits ou services reçus qui n'étaient pas ceux décrits sur le site Web; ou sommes supplémentaires retirées du compte sans autorisation. Les problèmes concernant les achats en ligne pouvaient être le résultat d'une erreur ou de moyens frauduleux.

Hameçonnage : A déjà reçu des courriels frauduleux d'une personne se faisant passer pour un représentant d'une organisation fiable et légitime, et demandant des renseignements personnels. Les autres types d'hameçonnage ne sont pas inclus dans le présent article.

Utilisateurs d'Internet : Aux fins du présent article, les utilisateurs d'Internet sont ceux qui ont déclaré avoir utilisé Internet dans les 12 mois précédant l'enquête.

Incidents autodéclarés de victimisation lies à la cyberintimidation d'adultes

Les courriels menaçants ou agressifs constituent la forme la plus courante de cyberintimidation

Lors de l'ESG, on a interrogé les répondants de 15 ans et plus sur leurs propres expériences de la cyberintimidation. De plus, on a demandé aux répondants de 18 ans et plus vivant avec des enfants de 8 à 17 ans dans leur ménage quelles avaient été les expériences de cyberintimidation de ces enfants. Pour éviter un chevauchement des données, la cyberintimidation des jeunes de 15 à 17 ans est analysée dans une section intitulée « Cyberintimidation et leurre d'enfants et de jeunes ».

Selon les résultats de l'ESG de 2009, 7 % des internautes de 18 ans et plus[3] ont indiqué qu'ils avaient déjà été victimes de cyberintimidation (tableau 1). La forme de cyberintimidation la plus souvent mentionnée concernait le fait de recevoir des courriels ou des messages instantanés menaçants ou agressifs, ce type d'incident ayant été signalé par les trois quarts (73 %) des victimes d'intimidation. La deuxième forme de cyberintimidation la plus commune concernait le fait d'être la cible de commentaires haineux, plus de la moitié (55 %) des victimes ayant déclaré de tels incidents. Enfin, moins de 1 victime sur 10 (8 %) a indiqué que quelqu'un avait envoyé des courriels menaçants en son nom.

Les utilisateurs de sites de réseautage social et de salons de clavardage sont deux fois plus susceptibles d'être victimes de cyberintimidation

Le risque de cyberintimidation[4] est aggravé par certaines caractéristiques de l'utilisation d'Internet, les plus notables étant l'utilisation de salons de clavardage ou de sites de réseautage social[5]. Les personnes qui utilisaient les salons de clavardage et les sites de réseautage social étaient presque trois fois plus susceptibles que les non-utilisateurs de faire l'objet de cyberintimidation (14 % et 11 % par rapport à 4 % et 3 %, respectivement) (tableau 3).

Les jeunes adultes, les célibataires, les homosexuels et les personnes ayant une limitation d'activité sont plus susceptible de faire l'objet de cyberintimidation

On a constaté que certaines caractéristiques sociodémographiques, comme le fait d'être jeune, célibataire, homosexuel ou bisexuel, ou d'avoir une limitation d'activité, avaient aussi pour effet d'augmenter le risque d'être victime de cyberintimidation. À titre d'exemple, les jeunes adultes entre 18 et 24 ans étaient proportionnellement trois fois plus nombreux que ceux de 25 ans et plus à indiquer avoir été victimes de cyberintimidation, soit 17 % contre 5 % (tableau 4).

De même, les célibataires étaient plus de trois fois plus susceptibles que les personnes mariées d'avoir subi de la cyberintimidation. Environ 15 % des utilisateurs d'Internet célibataires avaient été intimidés par rapport à 4 % des personnes mariées (y compris les conjoints de fait). Les utilisateurs d'Internet séparés ou divorcés étaient aussi plus susceptibles que les personnes mariées (ou vivant en union libre) de déclarer avoir été intimidés en ligne (9 % contre 4 %) (tableau 4).

Les répondants qui ont indiqué être homosexuels ou bisexuels étaient également proportionnellement plus nombreux à mentionner avoir fait l'objet de cyberintimidation, le pourcentage étant de deux à trois fois celui de leurs homologues hétérosexuels. Parmi les utilisateurs d'Internet, près du quart des personnes bisexuelles (24 %) et 1 personne homosexuelle sur 5 (18 %) ont été intimidées en ligne, comparativement à 7 % des hétérosexuels (tableau 5).

Enfin, les personnes ayant une limitation d'activité (c.-à-d. dont l'état physique ou mental ou un problème de santé de longue durée limite la quantité ou le genre d'activités auxquelles elles prennent part) étaient plus susceptibles de déclarer avoir été victimes de cyberintimidation (tableau 5). C'était particulièrement le cas des utilisateurs d'Internet de 18 à 34 ans. En effet, plus de 1 utilisateur d'Internet sur 5 (22 %) ayant une limitation d'activité avait été intimidé, comparativement à 10 % de ceux qui n'avaient aucune limitation.

Les victimes de crimes violents sont plus susceptibles de faire l'objet de cyberintimidation

L'ESG fournit aussi des renseignements sur les incidents de victimisation liés à des crimes violents (c'est-à-dire l'agression sexuelle, le vol qualifié et les voies de fait) qui se sont produits au cours des 12 mois précédant l'enquête. Les utilisateurs d'Internet qui ont indiqué avoir été victimes de crimes violents étaient plus susceptibles que ceux qui ne l'ont pas été de déclarer avoir aussi été victimes de cyberintimidation (20 % par rapport à 6 %) (tableau 4). Plus précisément, les victimes d'agression sexuelle, de vol qualifié de même que celles qui ont indiqué avoir fait l'objet d'au moins deux incidents violents étaient plus susceptibles d'avoir été intimidées en ligne; environ le tiers d'entre elles ayant affirmé avoir fait l'objet de cyberintimidation.

L'ESG ne permet pas de déterminer s'il y a un lien entre les incidents, mais d'autres études laissent entendre que les mêmes victimes sont souvent intimidées, tant dans le monde virtuel que dans le monde réel (Flores, 2005).

Les relations de confiance au sein de la famille offrent une protection contre la cyberintimidation

Alors que certaines caractéristiques font augmenter le risque de cyberintimidation, d'autres semblent l'atténuer. Par exemple, les internautes ayant indiqué qu'ils pouvaient avoir entièrement confiance dans les membres de leur famille[6] étaient moins susceptibles d'être intimidés en ligne que ceux qui ont affirmé pouvoir leur faire plus ou moins confiance (6 % par rapport à 13 %) (tableau 4). D'autres études montrent que le soutien familial et les relations positives aident à prévenir la cyberintimidation chez les enfants, du point de vu tant des victimes que des intimidateurs (Wienke Totura, 2009; Flores, 2005).

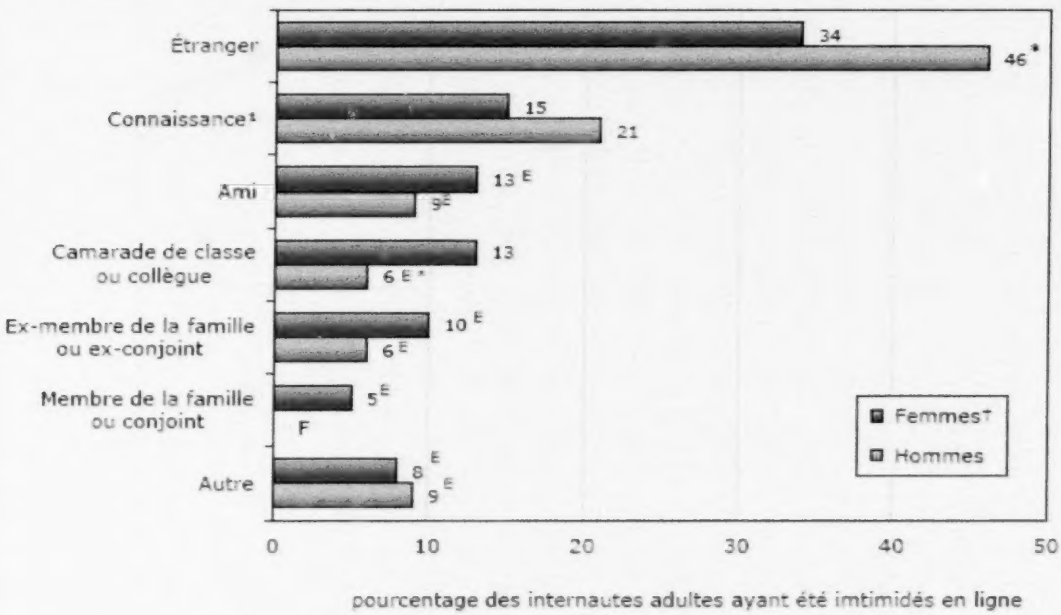
Les francophones[7] et les membres de minorités visibles étaient aussi moins susceptibles que leurs homologues de déclarer avoir été victimes de cyberintimidation. Environ 5 % des internautes francophones ont indiqué avoir été intimidés en ligne, par rapport à 8 % des internautes anglophones[8] (tableau 5). En ce qui concerne les membres de minorités visibles, même si la proportion ayant été intimidée était semblable à la proportion des personnes n'appartenant pas à une minorité visible (7 %), lorsque l'on tenait compte d'autres caractéristiques, comme l'âge, l'état matrimonial et l'utilisation de salons de clavardage ou de sites de réseautage social, on constatait que les internautes membres de minorités visibles étaient 30 % moins susceptibles d'avoir fait l'objet de cyberintimidation (tableau 9).

Les hommes sont plus susceptibles que les femmes d'être intimidés par un étranger

Dans l'ensemble, les hommes et les femmes, dans une proportion de 7 %, étaient tout aussi susceptibles d'avoir subi de la cyberintimidation (tableau 4). Toutefois, le lien entre la victime et l'agresseur différait légèrement selon le sexe de la victime. Les hommes étaient plus susceptibles que les femmes d'être intimidés par un étranger (46 % par rapport à 34 %). Bien qu'un tiers des femmes aient été intimidées par un étranger, elles étaient plus susceptibles que les hommes d'être intimidées par un camarade de classe ou un collègue (13 % contre 6 % pour les hommes) (graphique 1).

Les personnes de 25 ans et plus ayant fait l'objet de cyberintimidation étaient également plus susceptibles que les personnes entre 15 et 24 ans d'être intimidées par un étranger (49 % et 23 %, respectivement). Parmi ce groupe d'âge plus jeune, la plupart des personnes (64 %) avaient été intimidées par un ami, un camarade de classe ou une connaissance.

Graphique 1
Internautes adultes ayant déclaré avoir été victimes de cyberintimidation, selon le lien entre l'intimidateur et la victime, 2009



† catégorie de référence
E à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. Comprend les voisins, les connaissances, les amis sur Internet et les connaissances de vue seulement.
Note : Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut.
Source : Statistique Canada, Enquête sociale générale de 2009.

Relativement peu d'incidents de cyberintimidation sont signalés à la police

Les cas de cyberintimidation sont rarement signalés à la police, le taux s'élevant à moins de 1 incident de victimisation sur 10 (7 %) en 2010. Toutefois, comme tous les cas de cyberintimidation ne sont pas toujours de nature criminelle, et qu'ils ne justifient pas toujours le recours à la police, d'autres mesures peuvent être plus appropriées. Les victimes étaient plus enclines à bloquer les messages de l'expéditeur (60 %), à quitter le site Internet (51 %) ou à signaler l'incident à leur fournisseur de services Internet ou de courriel (21 %)[9].

Les femmes étaient plus susceptibles que les hommes de prendre des mesures pour faire cesser la cyberintimidation. Plus précisément, environ 7 femmes sur 10 (71 %) ont bloqué les messages de l'expéditeur responsable, et près du quart (23 %) ont signalé l'incident à leur fournisseur de services Internet ou de courriel. Dans le cas des hommes, les proportions s'élevaient à 49 % et 18 %, respectivement.

Encadré 2
Cybercrimes déclarés par la police

Certains services de police au Canada recueillent de l'information sur les cybercrimes. Ces données représentent les affaires qui sont venus à l'attention de la police et dont celle-ci a déterminé, dans le cadre d'une enquête, qu'Internet était l'objet du crime ou qu'un ordinateur avait été utilisé pour commettre l'infraction. En 2009, un sous-ensemble de services de police desservant 51 % de la population canadienne a fourni des données sur la cybercriminalité dans le Programme de déclaration uniforme de la criminalité (DUC).

Les données du Programme DUC révèlent que le sous-ensemble de services de police a déclaré 3 334 cybercrimes en 2009. De ces crimes, la fraude était l'infraction la plus courante; représentant plus de la moitié (55 %) de tous les cybercrimes. Les affaires d'intimidation[1] constituaient le quart (23 %) de ces affaires déclarées par la police, alors que le leurre d'enfants par Internet en représentait 7 %[2].

Le Programme DUC permet de recueillir certains renseignements sur les auteurs présumés d'infractions, pour ce qui est des crimes violents comme l'intimidation, il fournit également des données sur les victimes. Ces données indiquent que la plupart des victimes d'affaires de cyberintimidation déclarées par la police étaient des femmes ou des jeunes filles, soit environ 7 victimes sur 10 (67 %). Dans les cas de leurre d'enfants, environ 9 victimes sur 10 (90 %) étaient des filles.

Selon les renseignements de la police sur les affaires de cybercriminalité résolues, la plupart des auteurs présumés en 2009 étaient des hommes. Les personnes de sexe masculin étaient les auteurs présumés dans 72 % des affaires de cyberintimidation et dans la vaste majorité (98 %) des affaires de leurre d'enfants. L'âge médian des auteurs présumés de cyberintimidation se situait à 21 ans alors que les auteurs présumés de leurre d'enfants étaient un peu plus âgés, soit 33 ans. Alors que la plupart des victimes de cyberintimidation connaissaient l'auteur présumé (80 %), la plupart des victimes de leurre d'enfant avaient été attirées par un étranger (69 %).

1. Aux fins de la présente analyse, l'intimidation comprend les affaires d'extorsion, d'intimidation d'une personne non associée au système judiciaire, de harcèlement criminel, ainsi que les appels téléphoniques indécents ou harcelants et les menaces. L'information sur les victimes est recueillie seulement pour les crimes violents.
2. Les proportions sont fondées sur les réponses obtenues d'un sous-ensemble de services de police desservant 51 % de la population. Pour obtenir de plus amples renseignements sur les affaires de leurre d'enfants par Internet déclarées par tous les services de police, voir l'article de *Juristat* « Leurre d'enfants par Internet » (Loughlin et Taylor-Butts, 2009).
Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire (version 2.2).

Cyberintimidation et leurre d'enfants et de jeunes

Dans l'ESG de 2009, on a demandé aux répondants adultes si l'un des enfants âgés de 8 à 17 ans vivant dans leur ménage avait déjà été victime de cyberintimidation. Plus précisément s'il avait reçu des courriels ou des messages instantanés menaçants; s'il avait été la cible de commentaires haineux envoyés par courriel, messagerie instantanée ou affichés sur des sites Internet; ou si quelqu'un avait envoyé des courriels menaçants en son nom. On a aussi demandé aux répondants si l'un des enfants avait fait l'objet de leurre ou d'avances sexuelles sur Internet.

Dans le cas où au moins un des enfants avait été victime de cyberintimidation ou fait l'objet de leurre ou d'avances sexuelles sur Internet, on a demandé aux répondants des détails additionnels sur l'incident le plus récent et ce qui avait été fait pour y mettre fin. Parce qu'on demandait aux répondants de fournir des renseignements sur le plus récent incident de cyberintimidation ou de leurre, il est impossible d'examiner ces deux types de victimisation séparément lorsque les données sont analysées en détails. Il convient de mentionner que les données présentées dans cette section ne comprennent que les incidents dont le répondant adulte avait connaissance.

Environ 1 adulte sur 10 vivant dans un ménage où il y a des enfants indique qu'un enfant a été victime de cyberintimidation

Un peu moins de 1 adulte sur 10 (9 %) vivant dans un ménage où il y avait des enfants[10] avait connaissance d'un cas de cyberintimidation d'au moins un des enfants du ménage, une proportion qui était semblable dans toutes les régions du pays. Environ 15 % de ces adultes ont indiqué que plus d'un des enfants du ménage avait été la cible d'intimidation sur Internet. Un autre 2 % ont déclaré qu'au moins un de leurs enfants avait été leurré ou avait reçu des avances sexuelles sur Internet.

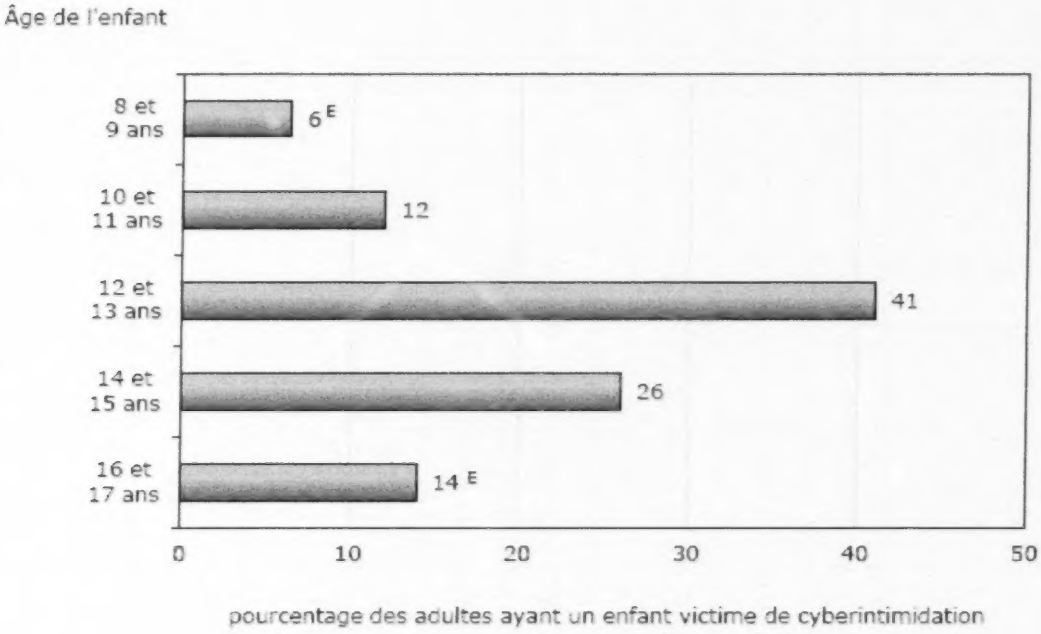
La forme de cyberintimidation des enfants la plus courante consistait à recevoir des courriels ou des messages instantanés menaçants ou agressifs, cette forme ayant été déclarée par 74 % des adultes qui avaient connaissance d'un tel incident dans leur ménage. Suivaient le fait d'avoir été la cible de commentaires haineux envoyés par courriel, messagerie instantanée ou affichés sur un site Internet (72 %); et l'envoi de courriels menaçants en utilisant l'identité de la victime (16 %)[11].

Les filles sont plus susceptibles que les garçons d'être intimidées sur Internet

Les résultats de l'ESG montrent que près des trois quarts (71 %) des adultes qui avaient connaissance d'un cas de cyberintimidation ou de leurre d'enfants ont indiqué que la victime était une fille. Cette proportion était la même, peu importe la façon dont l'intimidation ou le leurre avait été découverts (p. ex. si c'était l'enfant ou une autre personne, comme un responsable d'école, qui en avait informé le répondant).

Quatre adultes sur 10 (41 %) ayant un enfant victime dans leur ménage ont dit que cet enfant avait 12 ou 13 ans au moment de l'incident le plus récent (graphique 2). Cette constatation valait aussi bien pour les victimes de sexe féminin que masculin.

Graphique 2
Canadiens adultes ayant un enfant victime de cyberintimidation dans le ménage, selon l'âge de l'enfant au moment de l'incident le plus récent, 2009

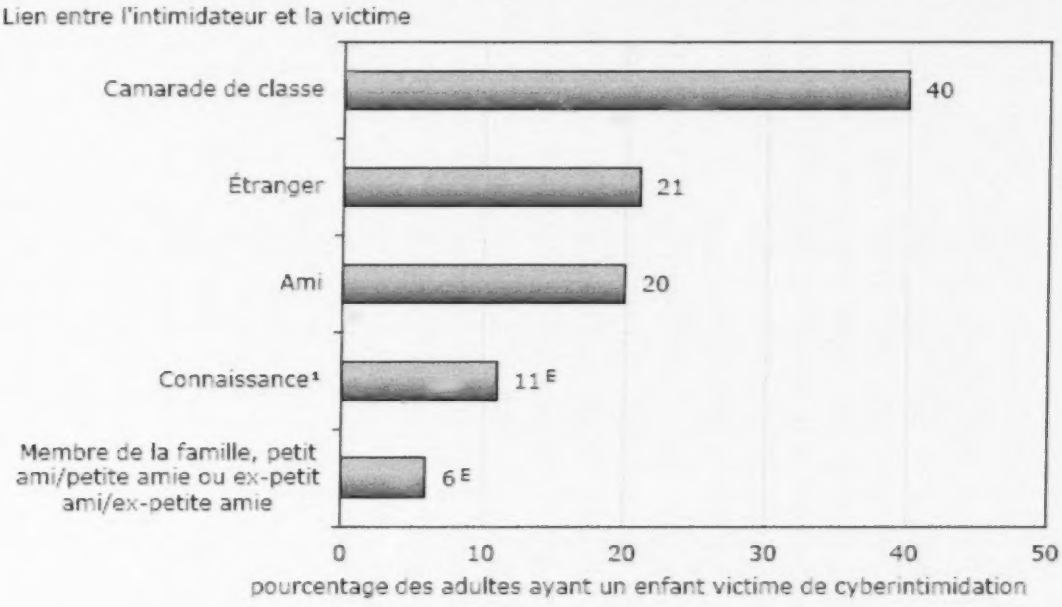


E à utiliser avec prudence
Note : Les données sont fondées sur l'information fournie par les répondants vivant avec au moins un enfant entre 8 et 17 ans. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut.
Source : Statistique Canada, Enquête sociale générale de 2009.

La plupart des victimes sont intimidées par une personne qu'elles connaissent

La plupart des adultes ont indiqué que les enfants avaient été intimidés par quelqu'un qu'ils connaissaient, habituellement un camarade de classe (40 %), un ami (20 %) ou une connaissance (11 %), plutôt qu'un étranger (21 %) (graphique 3). La seule exception concernait les cas de leurre d'enfants, pour lesquels 6 adultes sur 10 (60 %) ont précisé que l'enfant avait été attiré par un étranger[12].

Graphique 3
Adultes ayant un enfant victime de cyberintimidation dans le ménage, selon le lien entre l'intimidateur et la victime au moment de l'incident le plus récent, 2009



E à utiliser avec prudence
1. Comprend les voisins, les connaissances, les enseignants, les amis sur Internet et les connaissances de vue seulement.
Note : Les données sont fondées sur l'information fournie par les répondants vivant avec au moins un enfant entre 8 et 17 ans. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut.
Source : Statistique Canada, Enquête sociale générale de 2009.

Les incidents de cyberintimidation des enfants sont rarement signalés à la police

À l'instar des incidents de cyberintimidation des adultes, ceux commis contre des enfants ne sont habituellement pas signalés à la police. Selon les données de l'ESG de 2009, 14 % des incidents de cyberintimidation et de leurre d'enfants dont étaient au courant les adultes du ménage avaient été signalés à la police et un peu moins de 1 incident sur 10 (9 %) avaient été rapportés au fournisseur de services Internet ou de courriel, ou au site Web. Toutefois, comme l'ESG ne tient compte que des incidents d'intimidation sur Internet connus des adultes, la proportion réelle d'incidents portés à l'attention de la police est probablement encore plus faible.

Parmi les mesures prises pour mettre fin à la cyberintimidation ou au leurre, la plus courante consistait à bloquer les messages de l'expéditeur, cette mesure ayant été mentionnée par près des deux tiers (64 %) des adultes vivant dans un ménage où il y avait un enfant intimidé ou leurré. Dans presque la moitié des cas (47 %), l'accès de l'enfant à Internet ou au site en question avait été bloqué. De plus, environ le tiers (34 %) des adultes ont déclaré avoir communiqué avec les dirigeants de l'école pour demander de l'aide afin de remédier à la situation.

De surcroît, de nombreux adultes vivant avec des enfants de 8 et 17 ans disaient qu'ils imposaient des restrictions sur l'utilisation d'Internet dans leur ménage. Afin de protéger les enfants contre la cyberintimidation, 6 adultes sur 10 (59 %) ont indiqué limiter l'accès de leurs enfants à certains sites Internet, 58 % de ces adultes ayant recours à des logiciels de contrôle parental pour y parvenir.

Encadré 3
Cyberintimidation des adolescents de 15 à 17 ans — comparaison entre les incidents autodéclarés et ceux déclarés par les adultes

L'ESG de 2009 a servi à recueillir de l'information sur la cyberintimidation des jeunes de 15 à 17 ans de deux façons. On a questionné directement les répondants de 15 à 17 ans sur leurs expériences de cyberintimidation comme on l'a fait pour les répondants de 18 ans et plus. On a aussi posé aux répondants adultes ayant des enfants de moins de 18 ans dans le ménage des questions sur les expériences de cyberintimidation de ces enfants[1].

En général, les taux de cyberintimidation des jeunes de 15 à 17 ans qui ont été déclarés par les adultes étaient semblables à ceux fournis par ces jeunes eux-mêmes, ce qui suggère que bon nombre des incidents de cyberintimidation sont portés à l'attention des adultes du ménage. Plus précisément, 19 % des adolescents de ce groupe d'âge ont indiqué qu'ils avaient été victimes de cyberintimidation, alors qu'environ 12 % des adultes ayant au moins un adolescent de 15 à 17 ans dans le ménage ont dit qu'au moins un de ces jeunes avaient fait l'objet de cyberintimidation. De ces adultes, 15 % ont précisé que plus d'un adolescent du ménage avait été intimidé. Les réponses déclarées par les adultes et celles fournies par les jeunes étaient aussi très semblables en ce qui concerne le sexe des victimes et le lien entre celles-ci et l'intimidateur.

Lorsqu'on a interrogé les adultes sur l'incident de cyberintimidation le plus récent, environ 6 adultes sur 10 (62 %) ont indiqué que l'intimidation était survenue lorsque l'adolescent avait moins de 15 ans.

1. Dans la présente section, les chiffres concernant les adultes comprennent seulement ceux dont les enfants avaient entre 15 et 17 ans et qui n'avaient pas d'enfants entre 8 et 14 ans.

Incidents autodéclarés de victimisation liés à la fraude bancaire par Internet

La Colombie-Britannique et l'Ontario signalent les plus fortes proportions de victimes de fraude bancaire par Internet

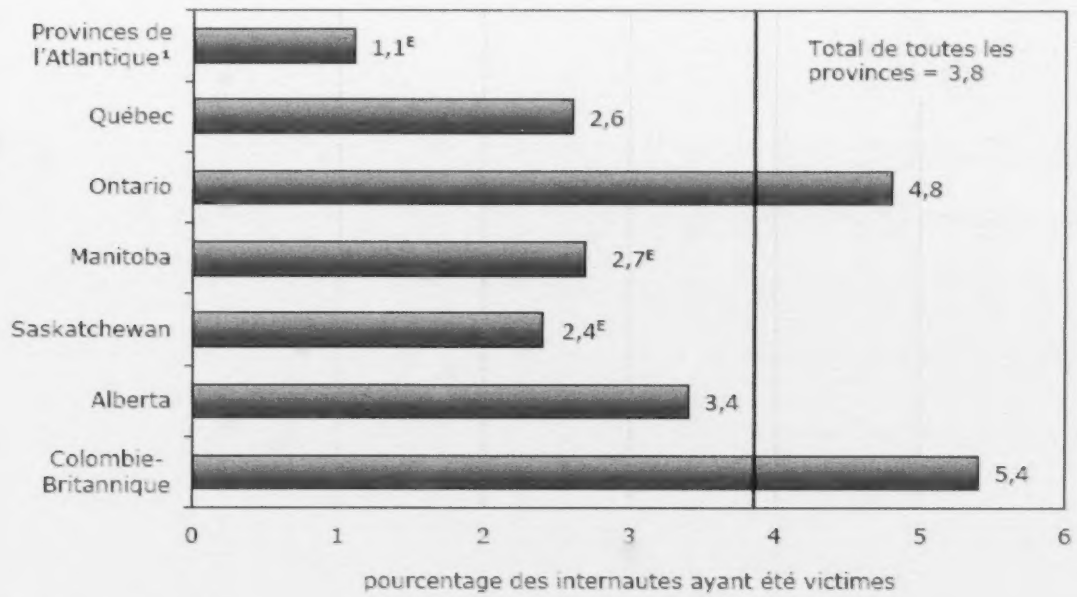
Selon les résultats de l'ESG de 2009, environ les deux tiers (64 %) des utilisateurs d'Internet ont indiqué être très préoccupés ou plutôt préoccupés par la sécurité des opérations bancaires sur Internet, même si plus des deux tiers (68 %) ont affirmé avoir effectué des opérations bancaires en ligne au moins occasionnellement.

Dans l'ensemble, 4 % des internautes ont déclaré avoir été victimes de fraude bancaire dans les 12 mois précédant l'enquête. Parmi les provinces, la Colombie-Britannique (5 %) et l'Ontario (5 %) ont enregistré les plus fortes proportions de victimes de fraude bancaire (graphique 4 et tableau 1).

La fraude bancaire par Internet est plus élevée dans les grandes régions métropolitaines du Canada

Les victimes de fraude bancaire sont plus susceptibles de vivre dans une région métropolitaine de recensement que dans toute autre région du pays. Environ 4 % des résidents de régions métropolitaines de recensement ayant utilisé Internet au cours de l'année précédente ont été victimisés, comparativement à 2 % des personnes vivant dans d'autres régions (tableau 2). Les proportions les plus élevées de victimes ont été constatées dans les régions métropolitaines de Toronto et Vancouver (7 % dans les deux cas).

Graphique 4
Internautes qui ont déclaré des incidents de victimisation de fraude bancaire par Internet, selon la province, 2009



[E] à utiliser avec prudence
1. Les provinces de l'Atlantique ont été groupées en raison des petits chiffres. Voir au tableau 1 les chiffres pour chacune des provinces.
Note : Les pourcentages sont fondés sur les Canadiens qui ont utilisé Internet au cours des 12 mois précédant l'enquête. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut.
Source : Statistique Canada, Enquête sociale générale de 2009.

L'utilisation fréquente d'Internet, un revenu élevé et un haut niveau de scolarité sont associés à la fraude bancaire par Internet

Comme pour la cyberintimidation, on a déterminé que certaines caractéristiques socioéconomiques et de l'utilisation d'Internet ont pour effet d'augmenter le risque de victimisation lié à la fraude bancaire par Internet. Cela s'applique aux personnes qui utilisent Internet fréquemment pour effectuer des opérations bancaires. Plus précisément, 5 % des personnes qui ont indiqué effectuer des opérations bancaires en ligne au moins une fois par semaine ont été victimes de fraude bancaire, soit plus du double de la proportion de personnes qui ont rarement ou jamais effectué leurs opérations bancaires en ligne[13] (2 %) (tableau 3).

Le risque de fraude bancaire par Internet chez les internautes a aussi tendance à s'accroître en fonction du revenu personnel et du niveau de scolarité. Ainsi, parmi les utilisateurs d'Internet, les personnes dont le revenu dépassait 60 000 $ étaient environ trois fois plus susceptibles que les personnes touchant un revenu inférieur à 20 000 $ d'être victimes de fraude bancaire (6 % par rapport à 2 %) (tableau 4).

Une répartition semblable a été observée pour ce qui est du niveau de scolarité. Les utilisateurs d'Internet titulaires d'un grade universitaire étaient environ cinq fois plus susceptibles de signaler des incidents de fraude bancaire que ceux qui n'avaient pas de diplôme d'études secondaires (5 % par rapport à 1 %) (tableau 4). Bien que les personnes ayant un revenu et un niveau de scolarité plus élevés aient tendance à effectuer plus d'opérations bancaires en ligne que leurs homologues, l'écart subsiste lorsque la fréquence d'utilisation d'Internet est prise en compte (tableau 8).

Les francophones ont moins tendance à être victimes de fraude bancaire par Internet

Si certaines caractéristiques augmentent le risque de victimisation par fraude bancaire, d'autres le diminuent. À titre d'exemple, les Canadiens qui ont indiqué parler français à la maison ont enregistré un pourcentage moins élevé de fraude bancaire par Internet que ceux qui parlaient une autre langue. Plus précisément, le risque d'être victime de fraude bancaire était 25 % moins élevé chez les francophones que chez les anglophones (tableau 8).

La différence peut s'expliquer en partie par le fait que plusieurs tentatives de fraude par Internet sont faites en anglais. À titre d'exemple, 43 % des anglophones ont indiqué avoir reçu des courriels frauduleux de la part de personnes qui se faisaient passer pour des représentants d'organisations fiables et légitimes demandant des renseignements personnels. La proportion correspondante constatée chez les francophones était de 25 % (tableau 6).

Problèmes concernant les achats en ligne

Les problèmes liés aux achats en ligne s'observent plus souvent en Alberta

Environ 14 % des internautes ayant effectué des achats en ligne au cours des 12 mois précédant l'enquête se sont heurtés à un problème quelconque, soit causé par une erreur ou des moyens frauduleux, pour au moins une de ces transactions. En général, la proportion de consommateurs en ligne qui ont déclaré des problèmes concernant des achats en ligne au cours des 12 mois précédant l'enquête variait peu d'une région à l'autre du pays (tableau 1). L'Alberta a affiché la plus forte proportion, soit près de 1 consommateur en ligne sur 5 (18 %), alors que Terre-Neuve-et-Labrador a enregistré la moins élevée (9 %) (tableau 1).

Effectuer des opérations seulement avec des organisations bien connues réduit le risque de problèmes liés aux achats en ligne

Le fait de s'adresser seulement à des organisations bien connues semble offrir une certaine mesure de protection contre les problèmes qui peuvent survenir en faisant des achats en ligne. Parmi ceux qui avaient pris de telles précautions, 13 % ont indiqué qu'ils s'étaient heurtés à des problèmes liés aux achats en ligne, proportion inférieure à celle enregistrée par les répondants qui ont dit ne pas avoir limité leurs achats aux organisations bien connues (20 %) (tableau 3).

Les immigrants et les membres de minorités visibles sont davantage à risque lorsqu'ils effectuent des achats en ligne

Les proportions d'immigrants et de membres de minorités visibles qui ont signalé des problèmes en ce qui a trait aux achats en ligne étaient plus élevées que celle déclarée par les autres Canadiens. En 2009, 21 % des membres de minorités visibles et 18 % des immigrants qui avaient effectué des achats en ligne ont mentionné de tels problèmes. Par comparaison, la proportion correspondante s'établissait à 13 % pour les non-immigrants et les personnes n'appartenant pas à une minorité visible (tableau 5).

Ces différences peuvent s'expliquer en partie par le fait que certains types de fraude visent les immigrants, par exemple, les fraudes liées au processus à suivre pour obtenir la citoyenneté ou d'autres documents liés à l'immigration.

Questions générales de sécurité sur Internet

Quatre internautes sur 10 ont subi une tentative d'hameçonnage

La tentative d'hameçonnage, soit le fait de recevoir des courriels frauduleux de quelqu'un se faisant passer pour un représentant d'une organisation fiable et légitime demandant des renseignements personnels, est l'un des problèmes de sécurité les plus fréquents pour les internautes canadiens. Plus précisément, près de 4 internautes sur 10 (39 %) ont indiqué avoir fait l'objet d'au moins une tentative d'hameçonnage. Comme c'est le cas pour d'autres problèmes de sécurité, cette proportion peut être plus élevée, compte tenu que ce ne sont pas tous les utilisateurs d'Internet qui savent qu'ils ont subi une tentative d'hameçonnage.

Certains internautes sont plus vulnérables que d'autres aux tentatives d'hameçonnage. Ainsi, en 2009, les internautes de sexe masculin (45 %) ont plus souvent déclaré avoir subi une tentative d'hameçonnage que les internautes de sexe féminin (33 %). De même, les internautes de 35 à 44 ans (44 %), ceux étant titulaires d'un grade universitaire (54 %), ceux ayant un revenu personnel supérieur à 100 000 $ (58 %) et ceux habitant dans une région métropolitaine de recensement (43 %) étaient plus susceptibles que les autres internautes de subir une tentative d'hameçonnage (tableau 6).

Comme pour la fraude bancaire par Internet, les internautes francophones (25 %) étaient proportionnellement moins susceptibles que les anglophones (43 %) ou les allophones[14] (36 %) de subir une tentative d'hameçonnage. Cela peut signifier que plusieurs tentatives d'hameçonnage sont effectuées en anglais (tableau 6).

Le risque d'hameçonnage est aussi plus élevé chez les personnes qui effectuent des achats en ligne. Près des deux tiers (66 %) des personnes ayant dit faire des achats en ligne au moins une fois par semaine avaient subi au moins une tentative d'hameçonnage, comparativement à moins du quart (24 %) des internautes qui faisaient rarement ou ne faisaient jamais d'achats en ligne (tableau 7).

Une infection par un virus, un logiciel espion ou un logiciel publicitaire est le problème de sécurité sur Internet le plus courant

Une infection par un virus, un logiciel espion ou un logiciel publicitaire était le type de problème de sécurité sur Internet le plus courant, près des deux tiers des internautes (65 %) ayant signalé un tel incident. Fait paradoxal, les utilisateurs qui avaient un programme antivirus (67 %) étaient plus susceptibles que ceux qui n'en avaient pas d'indiquer que leur ordinateur avait été infecté par un virus (45 %) (tableau 7). Toutefois, on n'a pas demandé aux répondants de l'ESG s'ils avaient installé leur programme antivirus avant que leur ordinateur soit infecté. Bien que certains utilisateurs puissent s'être procuré un programme antivirus après que leur ordinateur ait été infecté, il est possible que ceux qui avaient déjà un programme antivirus aient été plus conscients qu'un virus avait infecté leur ordinateur.

D'autres types de problèmes de sécurité ont été signalés moins souvent par les internautes. À titre d'exemple, 9 % des répondants ont mentionné que leur compte de courriel ou leurs fichiers d'ordinateur avaient fait l'objet de piratage informatique, alors que l'information personnelle de 4 % des internautes avait été rendue publique.

Bien que plusieurs utilisateurs d'Internet aient vécu une forme quelconque de problème de sécurité, la plupart d'entre eux prenaient des mesures de protection. La vaste majorité d'entre eux utilisaient un programme antivirus (91 %), faisaient affaire avec des organismes reconnus (84 %) et supprimaient régulièrement les courriels de source inconnue. Près des trois quarts (73 %) des utilisateurs Internet ont aussi déclaré supprimer régulièrement les fichiers Internet temporaires et les témoins Internet. Toutefois une plus faible proportion d'utilisateurs d'Internet (33 %) ont dit changer régulièrement leur mot de passe.

Promotion de la haine sur Internet

Un internaute sur 6 est déjà tombé sur du contenu faisant la promotion de la haine ou de la violence

À l'instar de la victimisation en général, certains groupes dans la population sont plus ou moins susceptibles de faire l'objet de discrimination ou d'un crime haineux en raison de leur origine ethnique, de leur religion ou de leur orientation sexuelle (Dauvergne et Brennan, 2011). Le même phénomène se produit sur Internet, certains groupes étant ciblés par des sites qui font la promotion de la haine ou de la violence.

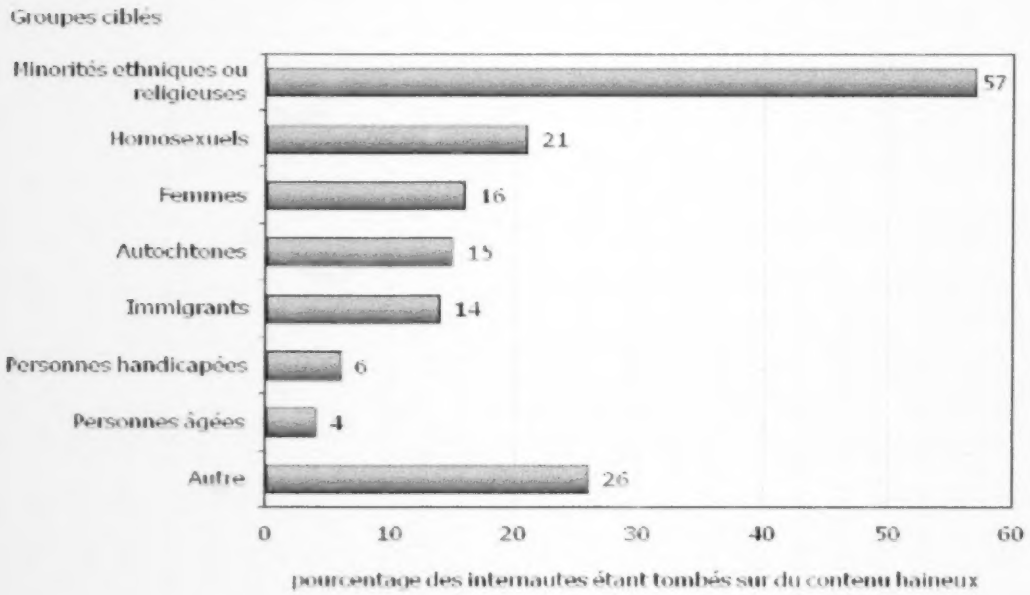
En 2009, près de 1 internaute sur 6 (16%) a déclaré être déjà tombé sur du contenu faisant la promotion de la haine ou de la violence envers un groupe particulier, qu'il l'ait cherché lui-même ou qu'il l'ait trouvé par inadvertance. Cependant, tous les répondants n'étaient pas susceptibles dans la même mesure de trouver du contenu haineux. Plus précisément, près de 1 jeune ou jeune adulte de 15 à 24 ans sur 3 (30 %) a déclaré avoir déjà trouvé du contenu haineux, soit plus du double de la proportion de ceux de 25 ans et plus (12 %) (tableau 6).

Les groupes ethniques ou religieux sont les cibles de contenu haineux sur Internet les plus souvent mentionnées par les internautes

On a demandé aux répondants de l'ESG de 2009 qui sont tombés sur du contenu haineux sur Internet de fournir des renseignements sur les groupes qui, selon eux, étaient visés. Ces résultats révèlent que les groupes ethniques ou religieux étaient les cibles de contenu haineux sur Internet les plus souvent signalées; ces groupes ont été mentionnés par plus de la moitié (57 %)[15] des internautes qui sont tombés sur du contenu haineux (graphique 5).

Ces résultats correspondent aux données sur les incidents perçus par les répondants comme étant des crimes haineux en général. Selon l'ESG de 2009, près des deux tiers (65 %) des crimes haineux déclarés par les répondants étaient, selon eux, motivés par la race ou l'origine ethnique, et 16 %, par la religion (Dauvergne et Brennan, 2011). Les internautes ont mentionné d'autres groupes qui étaient la cible de contenu haineux qu'ils ont trouvé sur Internet comme les homosexuels (indiqués par 21 % des internautes qui sont tombés sur du contenu haineux), les femmes (16 %), les Autochtones (15 %) et les immigrants (14 %) (graphique 5).

Graphique 5
Internautes étant tombés sur du contenu haineux sur Internet, selon le groupe ciblé par le contenu haineux, 2009



Note : Les pourcentages sont fondés sur les internautes qui sont tombés sur du contenu haineux au cours des 12 mois précédant l'enquête. Les catégories ne s'excluent pas mutuellement. Les répondants qui sont tombés sur du contenu faisant la promotion de la haine ou la violence envers un groupe donné pouvaient indiquer plus d'un groupe cible. Par conséquent, la somme des pourcentages ne correspond pas à 100. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut.
Source : Statistique Canada, Enquête sociale générale de 2009.

Résumé

En 2009, on a recueilli pour la première fois, dans le cadre de l'Enquête sociale générale (ESG) sur la victimisation, des renseignements sur les incidents de victimisation sur Internet liés à la cyberintimidation, à la fraude bancaire, et aux problèmes concernant les achats en ligne. Les données révèlent qu'environ 7 % des utilisateurs d'Internet adultes avaient été victimes de cyberintimidation, normalement aux mains d'un étranger ou d'une connaissance. De surcroît, environ 1 adulte sur 10 (9 %) ayant au moins un enfant entre 8 et 17 ans dans son ménage a affirmé qu'au moins un de ces enfants avait fait l'objet de cyberintimidation et 2 % ont rapporté un leurre d'enfants.

Les données de l'ESG ont également montré que 4 % des internautes ont été victimes de fraude bancaire. Parmi les Canadiens qui ont fait des achats en ligne au cours des 12 mois précédant l'enquête, 14 % se sont heurtés à un problème concernant au moins un de ces achats. Ceux qui ont fait des affaires seulement avec des organisations bien connues ont déclaré moins de problèmes concernant leurs achats en ligne que ceux qui n'ont pas pris ces précautions.

Méthode de l'analyse multivariable

Plusieurs facteurs peuvent être liés à un risque accru de victimisation sur Internet. Toutefois, la plupart de ces facteurs sont interdépendants. À titre d'exemple, les jeunes sont plus enclins que les adultes à utiliser des sites de réseautage social (comme Facebook et MySpace). Afin de déterminer lequel de ces facteurs a une plus grande incidence, ou plutôt, pour évaluer la mesure dans laquelle chaque facteur augmente ou diminue le risque de victimisation sur Internet, on a effectué une analyse multivariable. Par conséquent, un modèle de régression logistique est utilisé pour déterminer la contribution de chaque facteur à la victimisation. Ainsi, l'incidence de chaque facteur est évaluée alors que les autres facteurs sont maintenus constants. Cette incidence est exprimée sous forme d'un rapport de cotes.

Le rapport de cotes saisit la contribution au risque de victimisation par rapport à un groupe de référence. Un rapport de cotes qui est statistiquement significatif et supérieur à 1 indique que la caractéristique en question accroît le risque de victimisation. Un rapport de cotes qui est statistiquement significatif et inférieur à 1 indique que la caractéristique en question réduit le risque de victimisation. Le rapport de cotes exprime aussi le degré de risque accru. Par exemple, le modèle 1 (tableau 8) montre que la fréquence des opérations bancaires en ligne est le facteur qui présente le plus grand risque : les internautes qui effectuent des opérations en ligne tous les jours ont un risque de 2,25 fois supérieur à celui des internautes qui en font rarement ou jamais. À l'inverse, le risque de victimisation chez les francophones est d'environ 25 % inférieur (rapport de cotes de 0,72).

Méthode de l'Enquête sociale générale sur la victimisation

En 2009, Statistique Canada a réalisé le cycle de la victimisation de l'Enquête sociale générale (ESG) pour la cinquième fois. Les cycles précédents avaient été menés en 1988, 1993, 1999 et 2004. L'enquête vise à fournir des estimations des expériences personnelles qu'ont les Canadiens de huit types d'infractions, à examiner les facteurs de risque liés à la victimisation, à examiner les taux de déclaration à la police, à mesurer la nature et l'étendue de la violence conjugale, à mesurer la crainte de la criminalité et à examiner les perceptions du public à l'égard de la criminalité et du système de justice pénale. Pour la première fois, en 2009, l'ESG a aussi permis de recueillir des renseignements sur les expériences qu'ont eues les Canadiens de la victimisation sur Internet, c'est-à-dire de la fraude bancaire par Internet, de la cyberintimidation et des problèmes éprouvés en faisant des achats en ligne.

Échantillonnage

La population cible comprenait toutes les personnes de 15 ans et plus résidant dans les 10 provinces canadiennes, à l'exclusion des personnes vivant en établissement à temps plein. L'enquête a également été menée dans les trois territoires canadiens, les résultats pour ces régions étant prévus pour diffusion en 2011 dans un rapport séparé. On a choisi les ménages au moyen d'une méthode d'échantillonnage par téléphone appelée « composition aléatoire ». On a exclu de l'échantillon les ménages qui ne possédaient pas de téléphone et ceux qui utilisaient uniquement un téléphone cellulaire. Ces deux groupes ensemble représentaient environ 9 % de la population cible (Enquête sur le service téléphonique résidentiel, décembre 2008). Ainsi, la couverture pour 2009 s'élevait à 91 %.

Une fois qu'un ménage était choisi, une personne de 15 ans ou plus était sélectionnée au hasard pour participer à l'enquête. En 2009, l'échantillon comptait environ 19 500 ménages, un nombre moins élevé qu'en 2004 (24 000).

Collecte de données

La collecte de données s'est déroulée de février à novembre 2009 inclusivement. L'échantillon était réparti également sur les 10 mois afin que l'information représente les variations saisonnières. On s'est servi d'un questionnaire standard et l'on a recueilli les réponses dans le cadre d'interviews téléphoniques assistées par ordinateur. L'interview durait généralement 45 minutes. Avant la collecte, toutes les questions de l'ESG ont fait l'objet d'essais qualitatifs et d'essais pilotes.

Taux de réponse

Sur les 31 510 ménages choisis pour faire partie de l'échantillon du cycle 23 de l'ESG, 19 422 ont fourni des réponses exploitables, ce qui donne un taux de réponse de 61,6 %. Parmi les non-répondants, certains ont refusé de participer et d'autres ne pouvaient pas être joints ou ne parlaient ni français ni anglais. On a pondéré les chiffres des répondants de l'échantillon afin que leurs réponses représentent la population canadienne de 15 ans et plus vivant hors établissement dans les 10 provinces. Chaque personne qui a participé à l'ESG de 2009 représentait environ 1 400 personnes de 15 ans et plus dans la population canadienne.

Limites des données

Comme c'est le cas de toutes les enquêtes-ménages, les données comportent des limites. Les résultats reposent sur un échantillon et, par conséquent, ils sont sujets à des erreurs d'échantillonnage. Des résultats quelque peu différents auraient pu être obtenus si toute la population avait participé à l'enquête. Dans le présent *Juristat*, on emploie le coefficient de variation (CV) comme mesure de l'erreur d'échantillonnage. Toute estimation qui a un CV élevé (plus de 33,3 %) n'a pas été publiée parce qu'elle est trop peu fiable. Dans ces cas, on utilise le symbole « F » au lieu d'une estimation dans les graphiques et les tableaux de données. Lorsque le CV d'une estimation se situe entre 16,6 % et 33,3 %, il faut se servir de cette dernière avec prudence et on utilise le symbole « E ». Dans les cas où des statistiques descriptives et des analyses par recoupement ont été utilisées, les différences statistiquement significatives ont été déterminées en utilisant un intervalle de confiance de 95 %.

Dans le cas du plan d'échantillonnage et de la taille de l'échantillon de l'ESG de 2009, on s'attend à ce qu'une estimation d'une proportion donnée de la population totale, exprimée en pourcentage, se situe à 0,95 point de pourcentage de la proportion réelle 19 fois sur 20.

Notes

1. L'Enquête canadienne sur l'utilisation d'Internet (ECUI) et l'Enquête sociale générale (ESG) peuvent comporter des méthodes et concepts différents pour mesurer l'utilisation d'Internet. L'objectif principal de l'ESG est de mesurer la victimisation sur Internet. Par conséquent, les données suivantes sont basées sur les répondants de l'ESG ayant déclaré avoir utilisé Internet pendant les 12 mois précédant l'enquête.

2. Le présent rapport a été financé par le Centre de la politique concernant les victimes du ministère de la Justice Canada.

3. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, l'incident le plus récent de cyberintimidation aurait pu se produire avant que le répondant n'ait 18 ans.

4. Les éléments du risque et de la sécurité (à l'exception des facteurs géographiques) présentés dans cet article ont fait l'objet d'une analyse multivariable (régression logistique) afin de tenir compte de facteurs (comme la fréquence de l'utilisation d'Internet) qui peuvent avoir contribué au risque de victimisation. Seuls les facteurs qui sont statistiquement significatifs figurent dans le présent article. Pour obtenir de plus amples renseignements sur les résultats de l'analyse multivariable, voir Méthode de l'analyse multivariable.

5. À titre d'exemple de sites de réseautage social, mentionnons les sites MySpace et Facebook. À titre d'exemple de salons de clavardage, mentionnons les sites Yahoo Chat, PalTalk et ICQ.

6. Les réponses ont été fondées sur la question suivante : Quel degré de confiance accordez-vous aux gens de votre famille? On a utilisé une échelle à cinq notes, 1 représentant « On ne peut pas leur faire confiance du tout » et 5 représentant « On peut leur faire entièrement confiance ». Aux fins de la présente analyse, les réponses de 1 à 4 ont été regroupées dans la catégorie « On ne peut pas leur faire confiance du tout ou on peut leur faire plus ou moins confiance ».

7. Représente les personnes dont la langue la plus souvent parlée à la maison est le français.

8. Représente les personnes dont la langue la plus souvent parlée à la maison est l'anglais.

9. Les répondants pouvaient indiquer plus d'une mesure qu'ils ont prise pour mettre fin à la cyberintimidation.

10. Représente tous les répondants, y compris ceux qui ont déclaré que les enfants n'avaient pas utilisé Internet (4 % des répondants adultes vivant avec des enfants de 8 à 17 ans).

11. Comme les catégories ne s'excluent pas mutuellement, la somme des pourcentages peut ne pas correspondre à 100.

12. Les chiffres sont fondés sur les incidents dans lesquels un seul enfant du ménage avait été victime d'intimidation.

13. Un incident de fraude bancaire sur Internet peut se produire même si la victime n'utilise pas Internet pour faire ses opérations bancaires, puisque ces types d'incidents peuvent découler du vol d'identité ou du vol d'une carte de crédit ou de débit; il suffit qu'une source Internet ait été utilisée pour commettre la fraude.

14. Représente les personnes dont la langue parlée le plus souvent à la maison n'est ni l'anglais ni le français.

15. Les internautes pouvaient indiquer plus d'un groupe cible. Par conséquent, la somme des pourcentages ne correspond par à 100.

Références

CITOYENNETÉ ET IMMIGRATION CANADA. 2009. *Fraude en matière d'immigration — Protégez-vous!*, (consulté de 24 février 2011).

DAUVERGNE, Mia, et Shannon BRENNAN. 2011. « Les crimes de haine au Canada », *Juristat*, produit no 85-002-X au catalogue de Statistique Canada, (consulté le 13 juin 2011).

FLORES, Jasline, Marie-Marthe COUSINEAU et Nadia DESBIENS. 2005. *Mieux connaître et agir*, Centre québécois de ressources en promotion de la sécurité et en prévention de la criminalité.

GENDARMERIE ROYALE DU CANADA. 2011. « La fraude liée au magasinage en ligne concerne autant les acheteurs que les vendeurs », version mise à jour le 4 octobre 2010, (consulté le 31 mai 2011).

IPSOS REID. 2009. *Indice ACVM des investisseurs, 2009*, rapport établi à la demande du Comité de sensibilisation des investisseurs des Autorités canadiennes en valeurs mobilières, résumé, (consulté le 24 février 2011).

KOWALSKI, Melanie. 2002. *Cybercriminalité : questions, sources de données et faisabilité de la collecte de données auprès de la police*, produit no 85-558 au catalogue de Statistique Canada, (consulté le 9 août 2011).

LOUGHLIN, Jennifer et Andrea TAYLOR-BUTTS. 2009. « Leurre d'enfants par Internet », *Juristat*, vol. 29, no 1, produit no 85-002-X au catalogue de Statistique Canada, (consulté le 31 mai 2011).

MIDDLETON, Catherine, Ben VEENHOF et Jordan LEITH. 2010. *Intensité de l'utilisation d'Internet au Canada : comprendre les différents types d'utilisateurs*, produit no 88-006 au catalogue de Statistique Canada, Ottawa, « Division des enquêtes-entreprises spéciales et de la statistique de la technologie — Documents de travail », no 2, (consulté le 31 mai 2011).

MINISTÈRE DE LA JUSTICE CANADA. 2005. « Le Canada signe une entente internationale en vue de lutter contre les crimes racistes sur Internet », *Communiqués de presse*, le 8 juillet 2005, (consulté le 31 mai 2011).

PERREAULT, Samuel, et Shannon BRENNAN. 2010. « La victimisation criminelle au Canada, 2009 », *Juristat*, vol. 30, no 2, produit no 85-002-X au catalogue de Statistique Canada, (consulté le 31 mai 2011).

Sécurité publique. 2011. « La cybersécurité est l'affaire de tous au quotidien », http://www.securitepublique.gc.ca/prg/ns/cbr/index-fra.aspx (consulté le 9 août 2011).

Statistique Canada. 2011. « Enquête canadienne sur l'utilisation d'Internet, 2010 », *Le Quotidien*, mercredi le 25 mai 2011. (consulté le 9 août 2011).

WIENKE TORTURA, Christine, Carol MacKINNON-LEWIS, Ellis, L. GESTEN, Ray GADD, Katherine P. DIVINE, Sherri DUNHAM et Dimitri KAMBOULOS. 2009. « Bullying and Victimization Among Boys and Girls in Middle School, The Influence of Perceived Family and School Context », *Journal of Early Adolescence*, vol. 29, no 4, août 2009, p. 571 à 609.

WOLAK, Janis, David FINKELHOR, Kimberly J. MITCHELL et Michele L. YBARRA. 2008. « Online predators and their victims: Myths, realities and implications for prevention and treatment », *American Psychologist*, vol. 63, no 2, février-mars, p. 111 à 128.

Tableau 1
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon la province, 2009

	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
Provinces	**nombre (en milliers)**	**pourcentage[2]**	**nombre (en milliers)**	**pourcentage[2]**	**nombre (en milliers)**	**pourcentage[3]**
Terre-Neuve-et-Labrador	15[E]	5[E]*	F	F	15[E]	9[E]*
Île-du-Prince-Édouard	6[E]	7[E]	F	F	F	F
Nouvelle-Écosse	46	8	7[E]	1[E]*	38	12
Nouveau-Brunswick	25[E]	6[E]	F	F	31	14
Québec	259	5*	132	3*	281	12*
Ontario	621	7	428	5*	695	14
Manitoba	45[E]	6[E]	21[E]	3[E]	47	12
Saskatchewan	46	8	15[E]	2[E]*	49	15
Alberta	180	8	86	3	272	18*
Colombie-Britannique	253	8	175	5*	279	15
Total†	**1 494**	**7**	**872**	**4**	**1 709**	**14**

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
3. Les proportions sont fondées sur les internautes qui ont déclaré avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
Note : Le total exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 2
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon la région métropolitaine de recensement, 2009

Régions métropolitaines de recensement (RMR)[2]	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
	nombre (en milliers)	pourcentage[3]	nombre (en milliers)	pourcentage[3]	nombre (en milliers)	pourcentage[4]
St. John's	8[E]	6[E]	F	F	8[E]	10[E]*
Saint John	4[E]	5[E]	F	F	6[E]	14[E]
Halifax	22[E]	8[E]	F	F	21[E]	13[E]
Québec	29[E]	6[E]	F	F	26[E]	10[E]
Montréal	136	6*	72[E]	3[E]*	161	13
Ottawa–Gatineau	53[E]	7[E]	32[E]	4[E]	63[E]	11[E]
Toronto	263	7	265	7*	347	15
Hamilton	31[E]	7[E]	29[E]	6[E]	39[E]	15[E]
Kitchener–Cambridge–Waterloo	35[E]	11[E]	F	F	F	F
London	F	F	F	F	38[E]	19[E]
Winnipeg	25[E]	5[E]	14[E]	3[E]*	31[E]	12[E]
Regina	12[E]	9[E]	F	F	12[E]	16[E]
Saskatoon	12[E]	8[E]	F	F	16[E]	18[E]
Edmonton	62[E]	8[E]	37[E]	5[E]	104	21*
Calgary	79[E]	10[E]	20[E]	2[E]*	103	19
Vancouver	143	9	125	7*	168	16
Victoria	10[E]	4[E]*	F	F	26[E]	14[E]
Les 33 RMR†	**1 115**	**7**	**713**	**4**	**1 309**	**15**
Autres régions	**379**	**6***	**160**	**2***	**400**	**12***
Total	**1 494**	**7**	**872**	**4**	**1 709**	**14***

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Une région métropolitaine de recensement (RMR) est composée d'une ou de plusieurs municipalités voisines situées autour d'un noyau urbain. Une RMR doit compter au moins 100 000 habitants, dont au moins 50 000 vivent dans le noyau urbain. Pour faire partie de la RMR, les municipalités adjacentes doivent être fortement intégrées à la région urbaine centrale, le degré d'intégration étant mesuré par le débit de la migration quotidienne calculé à partir des données du recensement.
3. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
4. Les proportions sont fondées sur les internautes qui ont déclaré avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
Note : Les RMR pour lesquelles les données sont trop peu fiables pour être publiées ne sont pas affichées dans le tableau, mais leurs données figurent dans le calcul pour les 33 RMR. Le total exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 3
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon certaines caractéristiques de l'utilisation d'Internet, 2009

	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
Caractéristiques de l'utilisation d'Internet	**nombre (en milliers)**	**pourcentage[2]**	**nombre (en milliers)**	**pourcentage[2]**	**nombre (en milliers)**	**pourcentage[3]**
Fréquence des opérations bancaires en ligne						
Au moins une fois par semaine†	745	7	513	5	1 080	15
Au moins une fois par mois	280	8	131	4*	320	14
Occasionnellement	102[E]	8	57[E]	4[E]	87[E]	13[E]
Rarement ou jamais	336	6*	156	2*	195	9*
Fréquence des réservations en ligne						
Au moins une fois par semaine†	55[E]	7[E]	65[E]	8[E]	142	19
Au moins une fois par mois	374	7	309	6	630	14*
Occasionnellement	503	7	258	3*	620	14*
Rarement ou jamais	533	7	226	3*	294	12*
Fréquence des achats en ligne						
Au moins une fois par semaine†	110	11	74[E]	7[E]	235	22
Au moins une fois par mois	481	8	297	5	886	15*
Occasionnellement	468	7*	254	4*	463	11*
Rarement ou jamais	406	5*	232	3*	102[E]	11*
Utilisation de sites de réseautage social						
Oui†	1 144	11	471	4	1 154	17
Non	350	3*	402	4	554	11*
Utilisation de salons de clavardage						
Oui†	886	14	233	3	775	18
Non	609	4*	639	4	933	12*
Utilisation d'un logiciel antivirus						
Oui†	1 361	7	808	4	1 597	14
Non	104[E]	7[E]	61[E]	4[E]	105[E]	13
Transactions effectuées seulement avec des organisations biens connues						
Oui†	1 221	7	783	4	1 422	13
Non	265	9*	87[E]	3[E]*	281	20*
Changement régulier des mots de passe						
Oui†	596	8	327	4	673	15
Non	897	6*	545	4	1 032	13
Suppression régulière des courriels envoyés par des expéditeurs inconnus						
Oui†	1 335	7	771	4	1 587	14
Non	122[E]	7[E]	49[E]	3[E]*	95	12
Suppression régulière des fichiers Internet temporaires et des témoins Internet						
Oui†	1 222	8	686	4	1 430	15
Non	268	5*	181	3	265	11*

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
3. Les proportions sont fondées sur les internautes qui ont dit avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
Note : Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 4
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon les caractéristiques sociodémographiques et économiques des internautes, 2009

Caractéristiques sociodémographiques ou économiques	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[3]
Sexe						
Féminin†	751	7	402	4	719	13
Masculin	744	7	470	4	990	15*
Groupe d'âge						
15 à 24 ans[4]†	527	17	115[E]	3[E]	395	19
25 à 34 ans	388	9*	180	4	440	15*
35 à 44 ans	228	5*	213	5*	388	14*
45 à 54 ans	221	5*	186	4*	275	11*
55 à 64 ans	88	3*	133	4*	149	10*
65 ans et plus	42[E]	2[E]*	45[E]	3[E]	62	10*
État matrimonial						
Marié ou vivant en union libre†	582	4	606	4	1 032	13
Célibataire	776	15*	192	3*	569	17*
Séparé ou divorcé	121	9*	61[E]	4	101	16
Veuf	15[E]	4[E]	F	F	6[E]	4[E]*
Niveau de scolarité le plus élevé						
Université†	465	7	332	5	630	13
Collège ou école de métiers	352	5*	281	4	436	13
Études collégiales ou universitaires partielles	360	10*	144	4	363	18*
Diplôme d'études secondaires	229	8	79[E]	3[E]*	160	13
Sans diplôme d'études secondaires	87[E]	6	34[E]	1[E]*	115	14
Revenu personnel annuel						
Moins de 20 000 $†	512	11	133[E]	2[E]	485	18
20 000 $ à 39 999 $	342	7*	155	3	297	12*
40 000 $ à 59 999 $	242	6*	163	4*	287	12*
60 000 $ à 99 999 $	197	5*	224	6*	330	13*
100 000 $ ou plus	78[E]	5[E]*	103	6*	166	14*

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
3. Les proportions sont fondées sur les internautes qui ont dit avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
4. Pour la cyberintimidation des adultes, cette catégorie correspond aux personnes âgées de 18 à 24 ans.

Tableau 4 (suite)
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon les caractéristiques sociodémographiques et économiques des internautes, 2009

Caractéristiques sociodémographiques ou économiques	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[3]
Activité principale						
Exerce un emploi†	935	6	646	4	1 100	13
Est aux études	306	15*	63[E]	2[E]*	329	20*
Est à la recherche d'un emploi	49[E]	10[E]	F	F	39[E]	16[E]
Autre[5]	199	5*	153	3*	239	12
Consommation de drogues						
Ne consomme pas de drogue†	1 116	6	707	4	1 379	13
Régulièrement ou à l'occasion	372	13*	153[E]	5[E]	324	18*
Victimisation avec violence au cours des 12 mois précédant l'enquête[6]						
Aucun incident de victimisation avec violence†	1 202	6	789	4	1 484	13
Au moins un incident de victimisation avec violence	293	20*	84[E]	5[E]	225	23*
Un incident de victimisation avec violence	175	16*	66[E]	5[E]	166	22*
Deux incidents ou plus de victimisation avec violence	118[E]	31*	F	F	59[E]	27[E]*
Confiance dans les membres de la famille[7]						
On peut leur faire entièrement confiance†	1 253	6	771	4	1 528	14
On peut leur faire plus ou moins confiance	113[E]	13*	43[E]	4[E]	96	23*
On ne peut pas leur faire confiance du tout	126	11*	56[E]	5[E]	83[E]	13[E]

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
3. Les proportions sont fondées sur les internautes qui ont dit avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
4. Pour la cyberintimidation des adultes, cette catégorie correspond aux personnes âgées de 18 à 24 ans.
5. Comprend, par exemple, les répondants ayant déclaré être à la retraite, s'occuper des enfants, faire des travaux ménagers, être en congé de maternité ou de paternité, être en congé de maladie de longue durée, faire du bénévolat, ainsi que ceux ayant indiqué « Autre » à titre d'activité principale.
6. La victimisation avec violence comprend l'agression sexuelle, le vol qualifié et les voies de fait. Pour obtenir de plus amples renseignements sur la victimisation avec violence, voir Perreault et Brennan, 2010.
7. Les réponses étaient fondées sur la question suivante : Quel degré de confiance accordez-vous aux gens de votre famille? On a utilisé une échelle à cinq notes, 1 représentant « On ne peut pas leur faire confiance du tout » et 5 représentant « On peut leur faire entièrement confiance ». Aux fins de la présente analyse, les réponses de 2 à 4 ont été regroupées dans la catégorie « On peut leur faire plus ou moins confiance ».
Note : Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 5
Incidents de victimisation autodéclarés : cyberintimidation des adultes, fraude bancaire par Internet et problèmes concernant les achats sur Internet, selon certaines caractéristiques sociodémographiques et culturelles des internautes, 2009

Caractéristiques sociodémographiques ou culturelles	Cyberintimidation des adultes[1]		Fraude bancaire par Internet		Problèmes concernant les achats sur Internet	
	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[2]	nombre (en milliers)	pourcentage[3]
Immigrant						
Non†	1 225	7	667	4	1 267	13
Oui	264	6	204	4	438	18*
Membre d'une minorité visible						
Non†	1 289	7	715	4	1 375	13
Oui	198	7	144	4	326	21*
Identité autochtone						
Non-Autochtone†	1 425	7	851	4	1 667	14
Autochtone	63	10[E]	F	F	40	14[E]
Langue parlée à la maison						
Anglais†	1 159	8	662	4	1 305	14
Français	217	5*	115	3*	216	11*
Autre	118[E]	7[E]	96[E]	5[E]	188	21*
Orientation sexuelle[4]						
Hétérosexuel†	1 369	7	831	4	1 586	14
Homosexuel	45[E]	18[E]*	F	F	31[E]	19[E]
Bisexuel	56[E]	24[E]*	F	F	F	F
Limitation d'activité						
Aucune limitation†	916	6	612	4	1 195	13
Activités limitées	578	10*	259	4	511	17*

† catégorie de référence
[E] à utiliser avec prudence
F trop peu fiable pour être publié
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. La cyberintimidation des adultes comprend les répondants de 18 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, la période durant laquelle la cyberintimidation peut avoir eu lieu n'est pas limitée.
2. Les proportions sont fondées sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête.
3. Les proportions sont fondées sur les internautes qui ont dit avoir effectué des achats en ligne au cours des 12 mois précédant l'enquête.
4. On a posé la question sur l'orientation sexuelle seulement aux répondants de 18 ans et plus.
Note : Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 6
Internautes ayant déclaré des tentatives d'hameçonnage, des infections virales et du contenu haineux selon certaines caractéristiques sociodémographiques et culturelles, 2009

Caractéristiques sociodémographiques ou culturelles	Tentatives d'hameçonnage		Infections virales		Contenu haineux	
	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage
Sexe						
Féminin†	3 743	33	6 811	60	1 411	12
Masculin	5 151	45*	8 035	70*	2 142	19*
Groupe d'âge						
15 à 24 ans†	1 560	35	3 058	69	1 310	30
25 à 34 ans	1 895	43*	3 131	70	838	19*
35 à 44 ans	1 981	44*	3 024	68	564	13*
45 à 54 ans	1 809	39*	3 063	67	457	10*
55 à 64 ans	1 142	37	1 813	59*	290	9*
65 ans et plus	507	29*	756	43*	94	5*
Lieu de résidence						
Région métropolitaine de recensement (RMR)[1]†	6 834	43	10 759	67	2 750	17
Hors-RMR	2 061	30*	4 087	60*	803	12*
Niveau de scolarité le plus élevé						
Université†	3 597	54	4 675	70	1 170	18
Collège ou école de métiers	2 406	37*	4 220	65*	764	12*
Études collégiales ou universitaires partielles	1 479	41*	2 462	68	737	20
Diplôme d'études secondaires	782	25*	1 761	57*	364	12*
Sans diplôme d'études secondaires	602	21*	1 665	59*	512	18
Revenu personnel annuel						
Moins de 20 000 $†	2 051	33	3 990	65	1 402	23
20 000 $ à 39 999 $	1 687	34	3 050	62*	625	13*
40 000 $ à 59 999 $	1 548	38*	2 565	64	510	13*
60 000 $ à 99 999 $	1 844	50*	2 616	71*	570	15*
100 000 $ ou plus	924	58*	1 207	76*	236	15*
Immigrant						
Non†	6 924	38	11 843	65	2 875	16
Oui	1 955	42*	2 970	64	671	14
Membre d'une minorité visible						
Non†	7 472	39	12 576	65	2 997	15
Oui	1 334	42	2 154	67	540	17

† catégorie de référence
[E] à utiliser avec prudence
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
1. Une région métropolitaine de recensement (RMR) est composée d'une ou de plusieurs municipalités voisines situées autour d'un noyau urbain. Une RMR doit compter au moins 100 000 habitants, dont au moins 50 000 vivent dans le noyau urbain. Pour faire partie de la RMR, les municipalités adjacentes doivent être fortement intégrées à la région urbaine centrale, le degré d'intégration étant mesuré par le débit de la migration quotidienne calculé à partir des données du recensement.

Table 6 (suite)
Internautes ayant déclaré des tentatives d'hameçonnage, des infections virales et du contenu haineux selon certaines caractéristiques sociodémographiques et culturelles, 2009

Caractéristiques sociodémographiques ou culturelles	Tentatives d'hameçonnage		Infections virales		Contenu haineux	
	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage
Identité autochtone						
Non-Autochtone†	8 617	39	14 370	65	3 452	16
Autochtone	224	33*	400	59*	93	14
Langue parlée à la maison						
Anglais†	7 087	43	10 713	65	3 023	18
Français	1 116	25*	2 941	65	280	6*
Autre	691	36*	1 193	63	250	13*
Orientation sexuelle[2]						
Hétérosexuel†	8 261	40	13 391	65	2 984	15
Homosexuel	119	49	156	64	64[E]	26[E]*
Bisexuel	112	48	178	76*	51[E]	22[E]
Total	**8 894**	**39**	**14 846**	**65**	**3 553**	**16**

† catégorie de référence
[E] à utiliser avec prudence
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
2. On a posé la question sur l'orientation sexuelle seulement aux répondants de 18 ans et plus.
Note : Les proportions sont fondées sur tous les Canadiens ayant utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 7
Internautes ayant déclaré des tentatives d'hameçonnage, des infections virales et du contenu haineux, selon certaines caractéristiques de l'utilisation d'Internet, 2009

Caractéristiques de l'utilisation d'Internet	Tentatives d'hameçonnage		Infections virales		Contenu haineux	
	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage	nombre (en milliers)	pourcentage
Fréquence des opérations bancaires en ligne						
Au moins une fois par semaine†	5 032	50	7 054	69	1 795	18
Au moins une fois par mois	1 576	43*	2 573	70	672	18
Occasionnellement	500	32*	1 032	65*	287	18
Rarement ou jamais	1 692	25*	3 905	58*	769	12*
Fréquence des réservations en ligne						
Au moins une fois par semaine†	531	64	654	78	160	19
Au moins une fois par mois	2 977	54*	3 905	71*	1 064	19
Occasionnellement	3 116	42*	5 024	68*	1 203	16
Rarement ou jamais	2 194	26*	5 002	59*	1 102	13*
Fréquence des achats en ligne						
Au moins une fois par semaine†	705	66	787	74	286	27
Au moins une fois par mois	3 322	56*	4 314	73	1 332	23
Occasionnellement	2 811	41*	4 651	68*	1 010	15*
Rarement ou jamais	1 974	24*	4 828	58*	897	11*
Utilisation de sites de réseautage social						
Oui†	5 206	45	8 101	71	2 556	22
Non	3 687	32*	6 739	59*	996	9*
Utilisation de salons de clavardage						
Oui†	3 395	48	5 406	76	1 904	27
Non	5 494	35*	9 433	60*	1 647	11*
Utilisation d'un logiciel antivirus						
Oui†	8 310	40	14 015	67	3 271	16
Non	530	35*	677	45*	249	17
Transactions effectuées seulement avec des organisations biens connues						
Oui†	7 768	41	12 608	66	2 891	15
Non	1 073	32*	2 034	61*	645	19*
Changement régulier des mots de passe						
Oui†	3 374	44	5 149	67	1 444	19
Non	5 485	37*	9 612	64*	2 094	14*
Suppression régulière des courriels envoyés par des expéditeurs inconnus						
Oui†	8 331	43	12 981	68	3 201	17
Non	551	29*	1 137	60*	287	15
Suppression régulière des fichiers Internet temporaires et des témoins Internet						
Oui†	7 240	43	11 610	69	2 891	17
Non	1 565	29*	2 992	55*	639	12*
Total	**8 894**	**39**	**14 846**	**65**	**3 553**	**16**

† catégorie de référence
* différence significative par rapport à la catégorie de référence ($p < 0,05$)
Note : Les proportions sont fondées sur tous les Canadiens ayant utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les catégories de réponse « Ne sait pas » et « Non déclaré » sont comprises dans les totaux, mais elles ne figurent pas au tableau.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 8
Modèle 1 Régression logistique : risque de fraude bancaire par Internet, selon certaines caractéristiques des internautes, 2009

	Fraude bancaire
Caractéristiques des internautes	**rapport de cotes**
Revenu personnel	
100 000 $ ou plus	1,94***
60 000 à 99 999 $	2,02***
40 000 $ à 59 999 $	1,43*
Moins de 40 000 $	référence
Lieu de résidence	
Région métropolitaine de recensement	1,65***
Régions à l'extérieur des régions métropolitaines de recensement	référence
Niveau de scolarité le plus élevé	
Au moins des études partielles à l'école de métiers, au collège ou à l'université	1,73**
Diplôme d'études secondaires ou moins	référence
Langue parlée à la maison	
Langue non officielle	1.31
Français	0,73**
Anglais	référence
Fréquence des opérations bancaires en ligne	
Tous les jours	2,29***
Au moins une fois par semaine	1,53*
Au moins une fois par mois	1,24
Occasionnellement	1,4
Rarement ou jamais	référence

* différence significative par rapport à la catégorie de référence ($p < 0,05$)
** différence significative par rapport à la catégorie de référence ($p < 0,01$)
*** différence significative par rapport à la catégorie de référence ($p < 0,001$)
Note : Fondées sur tous les Canadiens de 18 ans et plus ayant utilisé Internet au moins une fois au cours des 12 mois précédant l'enquête. Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les variables non significatives ont été exclues du modèle. Celles-ci comprennent les suivantes : le sexe, l'âge, l'état matrimonial, l'activité principale, l'appartenance à une minorité visible, le statut d'immigrant, la consommation de drogues, la fréquence des réservations et des achats en ligne, les méthodes de protection (logiciel antivirus, changement des mots de passe), et l'utilisation de réseaux sociaux en ligne et de salons de clavardage.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 9
Modèle 2 Régression logistique : risque de cyberintimidation chez les adultes, selon certaines caractéristiques des internautes, 2009

Caractéristiques des internautes	Cyberintimidation rapport de cotes
Groupe d'âge	
18 à 24 ans	1,43*
25 ans et plus	référence
État matrimonial	
Célibataire	2,16***
Séparé ou divorcé	1,74***
Marié, vivant en union libre ou veuf	référence
Membre d'une minorité visible	
Membre d'une minorité visible	0,69*
Non-membre d'une minorité visible	référence
Langue parlée à la maison	
Langue non officielle	1,14
Français	0,61***
Anglais	référence
Orientation sexuelle[4]	
Homosexuel ou bisexuel	1,86**
Hétérosexuel	référence
Limitation d'activité	
Limitation d'activité	1,79***
Aucune limitation d'activité	référence
Utilisation de sites de réseautage social	
Oui	2,13***
Non	référence
Utilisation de salons de clavardage	
Oui	2,38***
Non	référence
Confiance dans les membres de la famille[1]	
On peut leur faire entièrement confiance	0,62***
On ne peut pas leur faire confiance du tout ou on peut leur faire plus ou moins confiance	référence
Victimisation avec violence dans les 12 mois ayant précédé l'enquête	
Deux incidents ou plus	3,22***
Un incident	1,63**
Aucun incident	référence

* différence significative par rapport à la catégorie de référence ($p < 0,05$)
** différence significative par rapport à la catégorie de référence ($p < 0,01$)
*** différence significative par rapport à la catégorie de référence ($p < 0,001$)
1. Les réponses étaient fondées sur la question suivante : Quel degré de confiance accordez-vous aux gens de votre famille? On a utilisé une échelle à cinq notes, 1 représentant « On ne peut pas leur faire confiance du tout » et 5 représentant « On peut leur faire entièrement confiance ». Aux fins de la présente analyse, les réponses de 1 à 4 ont été regroupées dans la catégorie « On ne peut pas leur faire confiance du tout ou on peut leur faire plus ou moins confiance ».
Note : Exclut les données du Yukon, des Territoires du Nord-Ouest et du Nunavut. Les variables non significatives ont été exclues du modèle. Celles-ci comprennent les suivantes : le sexe, le revenu personnel, l'activité principale, le niveau de scolarité, le lieu de résidence, le statut d'immigrant, l'identité autochtone, la consommation de drogues, le nombre d'amis proches vivant dans le quartier, la fréquence de l'utilisation d'Internet et les méthodes de protection (logiciel antivirus, changement des mots de passe).
Source : Statistique Canada, Enquête sociale générale de 2009.